NASPNCLAINST 5239.2B
Code 50000

NASPNCLA INSTRUCTION 5239.2B

Subj: DEPARTMENT OF THE NAVY AUTOMATED INFORMATION SYSTEMS (AIS's) SECURITY PROGRAM

Ref: (a) Public Law 100-235
(b) Public Law 98-473
(c) SECNAVINST 5239.2
(d) OPNAVINST 5239.1A
(e) CNETINST 5239.1A
(f) SECNAVINST 5870.5
(g) DODINST 5200.28
(h) CNATRAINST 5231.1C
(i) DODINST 5215.2
(j) CNATRAINST 5239.1B
(k) NASPNCLAINST 5231.2C

Encl: (1) Designated Approving Authority (DAA) Duties
(2) Information Systems Security Manager (ISSM)/Automated Data Processing Security Officer (ADPSO) Duties
(3) Information Systems Security Officer (ISSO)/Automated Data Processing Systems Security Officer (ADPSSO) Duties
(4) Terminal Area Security Officer (TASO) Duties
(5) Network Security Officer (NSO) Duties
(6) AIS Security Policy Statement
(7) Standard Operating Procedures
(8) NAS Pensacola’s AIS Security Briefing/Users Agreement/Authorization Form

1. Purpose

a. To establish the Department of the Navy (DON) Automated Information System (AIS) Security Program for Commander, Training Air Wing SIX; Naval Air Station Pensacola; and Training Squadrons FOUR, TEN, and EIGHTY-SIX. Hereinafter referred to as AIS users.

b. To set forth those policies and guidelines necessary for consistent and effective implementation.

c. To apply policy and principles of security as they relate to AIS's.

d. To implement references (a) through (k) and enclosures (1) through (8).

2. Cancellation. NASPNCLAINST 5239.2A

3. Scope. This instruction applies to all organizational components of Training Air Wing SIX (TW-6), NAS Pensacola, Training Squadron FOUR (VT-4), Training Squadron TEN (VT-10), and Training Squadron EIGHT-SIX (VT-86) and

addresses all elements of AIS security. All AIS's being developed, maintained, managed, operated, or used by these activities are covered by this instruction.

4. Objective. To provide centralized guidance and uniform policy on all aspects of AIS security. To ensure the availability of reliable information and automated support required to meet AIS user's missions. To establish and maintain an effective Risk Management Program and achieve accreditation for all AIS's, networks, and computer resources based on the results of the security accreditation process.

5. Policy. All AIS users having computer resources or designing computer applications will establish and maintain an AIS Security Program in accordance with this instruction and references (a) through (k), as applicable. Familiarization with reference (c) is necessary to implement Life Cycle Management (LCM), Accreditation, Risk Management, Contingency Planning, DAA, User Access, Security Implementation, and Interoperability. All Automated Data Processing (ADP) systems, office information systems, networks, and data they process will be protected in accordance with the appropriate directives and will be safeguarded by the continuous employment of protective features in all aspects of ADP Security.

6. Responsibilities

a. Designated Approving Authority (DAA). The DAA is responsible for ensuring compliance with the NATRACOM Computer Security Policy and Guidance. Enclosure (1) outlines the duties of the DAA. The DAA is responsible for TW-6, VT-4, VT-10, VT-86, and NAS Pensacola as directed by the TW-6 Commander. One AIS Security Plan should be developed to cover all assets and one will be assigned.

b. Information System Security Manager (ISSM)/Automated Data Processing Security Officer (ADPSO). The Management Information Systems Department staff (Code 50000) develops and manages the AIS Security Program with specific ISSM/ADPSO responsibility for the various staffs. The ISSM/ADPSO function resides in the Management Information Systems Office (MISO). The ISSM/ADPSO shall be appointed in writing with a copy to CNATRA Staff (Code 018). Enclosure (2) outlines ISSM/ADPSO duties.

c. Information Systems Security Officer (ISSO)/Automated Data Processing Systems Security Officer (ADPSSO). The Department Head appoints in writing the ISSO/ADPSSO to cover specific AIS's in each department. Enclosure (3) outlines specific responsibilities for the ISSO/ADPSSO.

d. Terminal Area Security Officer (TASO). The Department Head assigns TASO responsibility for remote computer terminals used by department personnel. Each area having one or more terminals has a TASO appointed. The TASO assignment can be the same as the ISSO/ADPSSO, provided the person is

working in the same area with the terminals. When the host computer is other than NAS Pensacola's, the host site can direct additional TASO responsibility. Enclosure (4) contains specific duties of TASO and TASO users.

e. Network Security Officer (NSO). The activity sponsoring network must assign an NSO for that network. A network for AIS security purposes includes more than one activity, each having operational control for one or more interconnected central computer systems. This interconnection of computers would exist in the day-to-day network operation. Enclosure (5) contains NSO duties.

f. AIS Computer User. A computer user is anyone who has access to or uses a computer. Users are responsible for complying with the Security Policies and Standard Operating Procedures contained in enclosure (6), (7), and (8).

g. Terminal User. A terminal user protects user ID and password from compromise. Terminal personnel use proper log on and log off procedures. Users log off terminals when finished and do not leave on-line terminals unattended.

(1) Personnel are responsible for using the terminal for authorized job-related projects only. Using terminals for personal gain is illegal and the unauthorized use of a Federal Government computer system is a violation of AIS security. This action may be interpreted as a criminal act, depending on the nature of the violation.

(2) Terminal users are responsible for protecting “Classified,” “Privacy Act,” and “For Official Use Only” information from unauthorized disclosure and identifying printed output appropriately.

7. Point of Contact. Naval Air Station Pensacola AIS Security Officer (Code 50B00), telephone 452-3798.

8. Forms. All forms mentioned in this instruction can be obtained from the ISSM/ADPSO.

J. M. DENKLER

Distribution:
B
COMTRAWING SIX
TRARON FOUR
TRARON TEN
TRARON EIGHT SIX

Stocked:
Commanding Officer
NAS Pensacola
190 Radford Blvd
Pensacola, FL 32508-5217

DESIGNATED APPROVING AUTHORITY (DAA) DUTIES

1. The DAA is responsible for ensuring compliance with the NATRACOM Computer Security Policy and Guidance.

2. The DAA will:

a. Be the final decision maker for violations of the AIS Security Policy within the command.

b. Appoint an ISSM/ADPSO in writing to act as a focal point for all AIS security matters.

c. Arrange training and career development of the ISSM/ADPSO, to include mandatory NCTS AIS Security Training.

d. Approve an Activity Automated Information Systems Security Plan (AAISSP).

e. Issue an IATO for a period not to exceed 1 year for any unaccredited operational system.

f. Accredit all systems operating under an IATO before placing new systems in user spaces.

g. Issue a "Statement of Accreditation" on each group of AIS's.

h. Ensure a continuing risk management and contingency plan program is in effect.

i. Issue written authorization for the use of privately owned AIS’s to conduct official DON business in a Department workplace or connected to a Navy or Marine Corps Network.

INFORMATION SYSTEMS SECURITY MANAGER (ISSM)/ AUTOMATED DATA PROCESSING SECURITY OFFICER (ADPSO) DUTIES

The ISSM/ADPSO will:

1. Implement and manage the AIS Security Program as prescribed by AIS Security directives and Public Laws.

2. Develop and maintain an AIS Security Plan. Update AIS Security Plan annually, at a minimum, to include any new AIS's.

3. Develop and maintain system accreditation support documentation (AIS Survey, risk assessment, contingency plan, security test, and evaluation) for AIS's. Accreditation must be according to the NATRACOM AIS Security System (NASS).

4. Accredit new AIS's before placing in the user spaces and reaccredit AIS's every 3 years, despite changes.

5. Ensure a Security Training and Awareness Program is in place to provide training for the security needs of persons accessing an AIS, network, or

computer resource. Use CNATRA 5239/5 for ISSO/ADPSSO attendance tracking. Maintain record of users trained using CNATRA 5239/6.

6. Advise and assist ISSO's/ADPSSO's when appropriate.

7. Coordinate with the Command Security Manager on matters concerning AIS security, according to the security organizational structure established by the Commanding Officer.

8. Appoint an NSO in writing for networks sponsored by the activity and ensure Department Heads appoint one or more ISSO/ADPSSO and/or TASO in writing.

9. Ensure all employees, civilian and military, comply with the Command Security Policy, enclosure (6), and Standard Operating Procedures, enclosure (7).

10. Provide ISSO/ADPSSO, TASO's, and NSO's a detailed listing of AIS's hardware and software for review, update, and verification annually at a minimum.

11. Notify the MISO in writing using NASP 5230/73 (Rev. 2-96) when the need arises to add hardware or software. Notify the Management Information Systems Department Trouble Call Desk at 2-4636 when the need arises to delete or move hardware or software. The MISO does all alterations of software and updates the master inventory listing and all software documentation.

12. Ensure all systems have an Authorized Users List posted.

13. Complete and maintain a copy of the AIS Security Incident Report if an AIS security incident occurs.

14. Prepare a Computer Security Technical Vulnerability Report according to reference (i) and Standard Operating Procedures (enclosure (8)) whenever a virus occurs.

15. Ensure AIS's have a DON approved Access Warning Screen and an activity standardized password program installed.

16. Ensure AIS's have the NATRACOM AIS Security Warning Poster in clear view and all hardware and software documentation are appropriately labeled.

17. Ensure users secure software documentation for AIS's to preclude theft. Check all hardware and software documentation for labels as described in enclosure (7).

18. Brief, indoctrinate, and train new and existing users regarding AIS security requirements.

19. Coordinate with the MISO on matters involving user-developed programs and AIS hardware/software inventory control.

20. Ensure users of assigned systems label reports containing "Privacy Act" or "For Official Use Only" information. If personal data or office-sensitive data resides on removable storage media, an external warning should indicate the medium contains "Privacy Act" or "For Official Use Only" information.

21. Maintain listing of systems processing "Privacy Act" or "For Official Use Only" information, and ensure users label reports properly.

22. Provide a written waiver to ISSO's/ADPSSO's for offices which cannot be locked

23. Ensure the network server, if any, is in a locked or controlled access area.

24. Ensure each AIS user has signed a copy of NAS Pensacola’s AIS Users Agreement, enclosure (8), prior to being allowed to access any AIS.

INFORMATION SYSTEMS SECURITY OFFICER (ISSO)/ AUTOMATED DATA PROCESSING SYSTEMS SECURITY OFFICER(ADPSSO) DUTIES

The ISSO/ADPSSO will:

1. Ensure all users of assigned AIS's, civilian and military, comply with enclosures (6), (7), and (8).

2. Review, update, and verify annually, the detailed listing provided by the ISSM/ADPSO of AIS's hardware and software.

3. Serve as the central point of contact for all requests from assigned users for additional training, hardware, and software.

4. Notify the MISO in writing (NASP 5230/73 Rev. 2-96) when the need arises to add hardware and software. Notify the Management Information Systems Department Trouble Call Desk at 2-4636 when the need arises to delete or move hardware or software. The MISO does all alterations of software and updates the master inventory listing and all software documentation.

5. Ensure there is an AIS Authorized User List for each AIS assigned and post. Update as required.

6. Complete the NATRACOM AIS Security Incident Report Form (CNATRA 5239/4) and forward to the ISSM/ADPSO if an AIS security incident occurs.

7. Assist ISSM/ADPSO by verifying assigned AIS's have a DON approved access warning screen and an activity standardized password program installed.

8. Verify assigned systems have the NATRACOM AIS Security Warning Poster in clear view and all hardware and software are appropriately labeled.

9. Secure software documentation for AIS's assigned to preclude theft. Check all hardware/software documentation for labels as described in enclosure (7).

10. Brief, indoctrinate, and train new and existing users regarding AIS security requirements.

11. Institute back-up procedures for AIS's assigned.

12. Turn off all stand-alone systems after each workday. Lock offices or obtain a written waiver from the ISSM/ADPSO for offices which cannot be locked.

13. Ensure users of assigned systems label reports containing "Privacy Act" or "For Official Use Only" information. If personal data or office sensitive data resides on removable storage media, an external warning should indicate the medium contains "Privacy Act" or "For Official Use Only" information.

14 Change all passwords at least every 180 days.

15. Ensure each AIS user in your department or activity signs a copy of NAS Pensacola’s AIS Users Agreement, enclosure (8), prior to being allowed to access an AIS.

TERMINAL AREA SECURITY OFFICER (TASO) DUTIES

The TASO will:

1. Be responsible for all AIS's and associated interface devices, including terminals, microcomputers, and microcomputers used as terminals, as assigned by the ISSO/ADPSSO.

2. Monitor the compliance of host computer security requirements set up by ISSM/ADPSO for remote terminal areas.

3. Maintain liaison with host computer ISSM/ADPSO or site coordinator to ensure continued security for assigned terminals.

4. Ensure terminal users are aware of their security responsibilities.

5. Ensure new users are given user logins and initial password assignments by the ISSM/ADPSO. If a group of employees use the same password, do not compromise password.

6. Not store the log-on validation sequence, including the password required by a large system in the microcomputer when the micro accesses a large central computer via terminal emulation.

7. Not process classified data on any computer system through remote terminals without obtaining proper authorization.

8. Ensure all users of assigned terminals, civilian and military, comply with enclosures (6), (7), and (8).

9. Assist ISSO/ADPSSO by reviewing, updating, and verifying annually, the detailed listing provided by the ISSM/ADPSO of terminal hardware and software.

10. Assist ISSO/ADPSSO by identifying all assigned user requests for training, hardware, and software.

11. Notify the MISO in writing (NASP 5230/73 Rev. 2-96) when the need arises to add hardware or software. Notify the Management Information Systems Department Trouble Call Desk at 2-4636 when the need arises to delete or move

hardware or software. The MISO does all alterations of software and updates the master inventory listing and all software documentation.

12. Ensure there is an AIS Security Users List for each assigned terminal and post.

13. Complete the NATRACOM AIS Security Incident Report Form (CNATRA 5239/4) and forward to the ISSM/ADPSO if an AIS security incident occurs.

14. Assist ISSO/ADPSSO by verifying assigned terminals have a DON approved access warning screen and an activity standardized password program installed.

15. Verify assigned terminals have the NATRACOM AIS Security Warning Poster in clear view and all hardware and software are appropriately labeled.

16. Secure software documentation for terminals assigned to preclude theft. Check all hardware and software documentation for labels as described in enclosure (7).

17. Brief, indoctrinate, and train new and existing terminal users/operators regarding terminal security requirements.

18. Institute back-up procedures for AIS's assigned.

19. Ensure terminals are properly logged off when operating personnel are not in the terminal area. Secure all terminals at end of each workday.

20. Distribute computer printed reports only to authorized individuals and label reports containing personal information properly (Privacy Act Information). If personal or office-sensitive data resides on removable storage media, an external warning should indicate the medium contains "Privacy Act" or "For Official Use Only" information.

21. Change all passwords as required and at least every 180 days.

NETWORK SECURITY OFFICER (NSO) DUTIES

The NSO will:

1. Include countermeasures and requirements in the network design. Ensure individual nodes of the network comply with these measures before interfacing with the network.

2. Ensure Network DAA and AIS activity DAA of the network node agree to security requirements in writing. Take this action before connecting the node to the network.

3. Develop and promulgate the standard security procedures governing network operations. Coordinate these procedures with the ISSM/ADPSO.

4. Ensure security measures and procedures used at network nodes fully support the security integrity of the network. Use all required countermeasures.

5. Maintain liaison with the MISO and ISSO's/ADPSSO's of the network.

6. Ensure all users of assigned AIS's, civilian and military, comply with enclosures (6), (7), and (8).

7. Review, update, and verify annually, the detailed listing provided by the ISSM/ADPSO of AIS's hardware and software.

8. Notify the MISO in writing (NASP 5230/73 Rev. 2-96) when the need arises to add hardware or software. Notify the Management Information Systems Department Trouble Call Desk at 2-4636 when the need arises to delete or move hardware or software. The MISO does all alterations of software and updates the master inventory listing and all software documentation.

9. Ensure there is an AIS Security User List for each AIS assigned and post. Update list as required.

10. Complete the NATRACOM AIS Security Incident Report Form (CNATRA 5239/4) and forward to the ISSM/ADPSO if an AIS security incident occurs.

11. Assist the ISSM/ADPSO by verifying assigned AIS's have a DON approved access warning screen and an activity standardized password program installed.

12. Verify assigned systems have the NATRACOM AIS Security Warning Poster in clear view and all hardware and software are appropriately labeled.

13. Secure software documentation for AIS's assigned to preclude theft. Check all hardware/software documentation for labels as described in enclosure (7).

14. Brief, indoctrinate, and train new and existing users regarding network security requirements.

15. Institue back-up procedures for the network.

16. Distribute computer-printed reports only to authorized individuals and label reports containing personal information properly (Privacy Act Information). If personal or office-sensitive data resides on removable storage media, an external warning should indicate the medium contains "Privacy Act" or "For Official Use Only" information.

17. Change passwords as required and at least every 180 days.

AIS SECURITY POLICY STATEMENT

With today's increased dependency on Automated Information Systems (AIS’s), we must make every effort to protect the integrity of the information stored on our systems. Adequately safeguard hardware and software for their intended operational support mission. Accordingly, to ensure compliance with all AIS Security directives and Public Laws, the following guidelines are established:

1. Do NOT copy proprietary software.

2. Do NOT use pirated software on government computers.

3. Do NOT allow games or any entertainment programs on government computers.

4. Do NOT allow personally owned hardware and software in government buildings without written authorization from the DAA.

5. Do NOT allow public domain or shareware software on government computers unless the software has been registered and scanned by an approved virus detection program.

6. A Password/Audit Trail Program will be installed on all government microcomputers.

7. All original software disks will be stored in one centralized library maintained by the MISO.

8. All software documentation will be labeled with appropriate system-ID.

9. Only data disks will be located in user spaces.

10. All departments/activities must set up a back-up program for any data.

11. Permit downloading programs from Government Bulletin Boards to a floppy disk if the program is necessary to job function and the ISSM/ADPSO completes a virus check. The MISO places program in the master inventory and the NATRACOM Custom Developed Software Catalog.

12. All systems will be fully accredited by the DAA or have a DAA issued IATO until accreditation can be accomplished before installation in users spaces.

13. Exportation of any hardware or software to other activities must be coordinated with the MISO.

14. Government-owned computers and software programs will not be used for personal or private business.

15. Do NOT allow eating or drinking in the immediate work area where equipment is located or operated. Allow no smoking in the same room with computers.

16. No microcomputer should be operated in temperatures greater than 85 degrees.

17. All military and civilian personnel will attend ADP Security Awareness Training annually.

18. All systems will have a DON approved Access Warning Screen installed.

19. All systems will have the NATRACOM Warning Poster displayed.

20. All system users will comply with enclosures (6), (7), and (8).

Abiding by the above policy will ensure compliance with the Public Laws and directives governing AIS Security. Failure to comply with Public Law is a federal offense carrying criminal penalties, including fines and imprisonment. To ensure the command incurs no liability, violation of the above policy will be reported by the ISSM/ADPSO to the DAA via supervisory chain of command. Violations may result in disciplinary action; i.e., verbal and/or written reprimand from the DAA; access denial to computer, etc.

STANDARD OPERATING PROCEDURES

1. General Policies

a. A copy of these procedures will be readily accessible for users of each Automated Information System (AIS).

b. All users will be instructed in the proper care and use of ADP equipment, storage media, and software per manufacturers instructions.

c. All users will be required to attend ADP Security Awareness Training.

d. All systems which process sensitive or classified material will have password/audit trail protection.

e. All systems will have a DON approved Warning Screen installed.

f. Disks or tapes shall be sufficiently secured to prevent unauthorized access or use.

g. AIS's processing Level I data must operate in accordance with OPNAVINST C5510.93E (NOTAL).

h. Do NOT allow program disks in user spaces. All software will be installed by MISO personnel and the original program disk stored in the centralized library.

2. Standards

a. Environmental Controls

(1) All computers will have an AIS Security Warning Poster in clear view.

(2) Do NOT allow eating or drinking in the immediate work area where equipment islocated or operated. Allow no smoking in the same room with computers.

(3) No microcomputer should be operated in temperatures greater than 85 degrees.

(4) Users should be aware of the closest fire extinguisher.

(5) A surge protection device should be used on all computers and all users should turn off and unplug their systems during thunderstorms.

(6) Equipment exposed to water will not be activated until inspected by qualified personnel.

(7) Provide plastic sheets to protect ADP equipment which is susceptible to water damage or dust.

b. Hardware

(1) No privately owned hardware will be used by AIS users unless given written approval by the DAA.

(2) No classified data will be processed on privately owned computers used in the government workplace.

(3) All Central Processing Units (CPU's) shall have an "Unclassified," "Sensitive Unclassified," or "Classified" label attached, depending on the highest level of information processed.

(4) Notify the MISO Trouble Call Desk at 2-4636 to have microcomputer or peripheral equipment relocated.

(5) If problems occur, users should contact the MISO Trouble Call Desk at 2-4636.

(6) Maintenance or modifications to systems will be done by the MISO personnel.

(7) AIS's will be located in offices or buildings that can be secured to prevent unauthorized removal or use.

c. Software

(1) Games. Do NOT allow games or any entertainment programs on any government computer.

(2) Personally Owned Software. Do not allow personally owned software in government buildings.

(3) Bulletin Board Software

(a) Prohibit downloading from commercial bulletin boards because of the high occurrence rate of viruses in bulletin board software.

(b) Permit downloading from Government Bulletin Boards to a floppy disk if the program is necessary to do job function. The ISSM/ADPSO completes a virus check before installing program. The MISO places program in the command master inventory and the NATRACOM Custom Developed Software Catalog before installation of program.

(4) Copying of Software

(a) Do NOT allow copying of proprietary software except as authorized by the manufacturer.

(b) Government-owned software will NOT be copied for personal or private use.

(5) Pirated Software. No pirated software will be used on any government computer.

(6) Public Domain or Shareware. Do NOT allow public domain or shareware on government computers unless the software has been registered and scanned by an approved virus detection program.

d. Storage Media

(1) Give particular attention to protection of magnetic media, as it is the primary means of data storage.

(2) Floppy Disks

(a) All data disks will be labeled with the highest level of data contained on the disk.

(b) Store in protective jacket.

(c) Protect from bending or similar handling.

(d) Avoid temperature extremes.

(e) Avoid contact with magnetic fields such as magnetic memo holders, magnetized paper clips, telephone handsets, etc.

(f) Do not write on diskette, either directly or through the jacket.

(g) Do not touch the exposed areas of the diskette. Fingerprints leave oily residue and could render data inaccessible.

(3) Fixed Disks

(a) Rough handling will damage the drive read/write heads.

(b) Use "Ship" or "Park" procedures before moving the CPU. This places the read/write heads in a "safe" area.

e. Back-up Procedures

(1) Backup all data to prevent loss if catastrophic system failure occurs. Microcomputer users will:

(a) Backup data files weekly where appropriate.

(b) Do system backups monthly.

(2) Magnetic media (disks, diskettes, tapes) containing sensitive information shall be cleared by degaussing before reuse or disposal.

f. Access

(1) Access to AIS's will be physically limited to authorized users.

(2) Restrict physical access to data files and media libraries to individuals requiring access to do official duties.

(3) No sensitive information should be transmitted using off site computing via modem to a government computer. An interactive security measure such as dial-back should be used to protect against illegal entry to the AIS.

(4) Disks/Tapes containing sensitive data shall be secured when not in use.

g. Password Procedures

(1) Passwords shall be protected to prevent unauthorized personnel from obtaining them. Passwords will be changed as required.

(2) Password change on a system will occur in the event of recognized compromise by unauthorized user.

h. Movement of Hardware/Software

(1) Any movement of computers will be done by MISO personnel. Notify the MIS Department Trouble Call Desk at 2-4636. An ADP Support Request (NASP 5230/73 (Rev. 2-96)) should be sent to the MISO for the addition, deletion, or change of software.

(2) Off Base/Off Staff. When removing government hardware/software

and resources from the office or using a personal off site computer, complete a Property Pass (NAVSUP Form 155). A copy of the form should be maintained by both ISSM/ADPSO and ISSO/ADPSSO.

(3) Provided by Outside Command. User should notify the MISO upon receipt of hardware/software. The MISO/designated person will enter the material into the master inventory, provide appropriate labels, and install the hardware/software.

(4) Delivery to another Command. User contacts the MISO before any software or hardware deliveries occur. This office coordinates the move through the receiving activity’s MISO.

i. Microcomputer Virus Control

(1) Preventive Measures

(a) Install the NATRACOM standard Virus Protection Program on all machines.

(b) Check all new software through the command MISO before installation. This routine should involve, at least, a search for bad sectors, a review of the boot sector, and a review of READ.ME files using a special editor. Never use a DOS type command to do this.

(c) Make backups regularly. Backup data from interactive systems more frequently than others.

(d) Keep master diskettes secure. When adding a new software program to the system, write-protect the diskette containing the program before inserting it into the disk drive. This means covering the notch on the upper right side of a 5 1/4 inch diskette with a write-protect tab. With a 3 1/2 inch disk, the plastic square in the upper right-hand corner should be shifted so one may look through the hole.

(e) Maintain regular checkups of a network. The network administrator should control all software programs put on the network. The transfer of any executable program over the network should be controlled. These transfers should be eliminated whenever possible. There is a greater danger for the spread of a virus over the network than the physical handling of diskettes. More testing and precautions are essential in a networked computing environment.

(f) Do NOT share program disks or software between systems.

(g) Verify sizes of files and periodically recheck.

(h) Follow command policy regarding use of public domain, shareware, games, illegal software, and downloading from bulletin boards.

(2) Virus Symptoms

(a) Files mysteriously appear or disappear.

(b) Unexplained changes in data.

(c) Disk fills up faster than normal.

(d) Memory capacity is used.

(e) Unusual screen messages.

(3) Procedures When Virus is Found

(a) DO NOT turn off the machine.

(b) Isolate at once any system which has been infected with a virus.

(c) Stop all processing on the system or network.

(d) Notify immediately the ISSM/ADPSO.

(e) The ISSM/ADPSO will:

1. Conduct a preliminary investigation.

2. Notify the appropriate ISSO/ADPSSO to collect all floppy disks, including any back-up disk and run the NATRACOM Virus Clean Program against the diskette.

3. Turn the preliminary investigation report over to the Naval Investigation Service for their action if cost estimate is more that $500.

4. Prepare a Computer Security Technical Vulnerability Report and forward to Commander, Naval Computer and Telecommunications Command, according to DODINST's 5215.2 and 5200.28.

5. Notify user and appropriate ISSO/ADPSSO when system may be used.

j. AIS Security Violation Reporting

(1) Examples of AIS Security Violations

(a) Loss of hardware, software, documentation.

(b) Violation of copyright laws concerning proprietary software applications.

(c) Disclosure (intentional or unintentional) of sensitive unclassified or classified data.

(d) Unexplained loss of data or malfunction of an AIS.

(e) Unauthorized access to systems or data by personnel without proper clearance or need to know.

(2) Who Reports? Anyone can identify an AIS Security Violation.

(3) To Whom and How is an AIS Security Violation Reported?

(a) AIS security violations should be reported directly to the ISSM/ADPSO.

(b) The ISSM/ADPSO works with and coordinates any security investigations with the Command Security Manager. If the ISSM/ADPSO determines in the preliminary investigation that classified material may have been compromised, the command must notify the Naval Investigative Service (NIS) who conducts a formal investigation. Also, notify NIS if fraud, abuse, or criminal actions are discovered.

(c) The ISSM/ADPSO is responsible for:

1. Beginning the preliminary investigation while details are still fresh in everyone's minds.

2. Securing the system(s) involved to preserve any evidence of tampering or to prevent the spread of the potential problem to other systems or data files.

3. Reviewing all system audit or access logs to find the events leading to the problem and to identify personnel having access to the system at the time the security incident occurred. Save all audit records.

4. Interviewing all personnel who may have information concerning the cause of the security incident.

5. Documenting the investigation and maintaining all documentation of the preliminary investigation. This information includes audit trails, hardcopy information from the system or network, any media considered as evidence, and personnel interview notes.

6. Reporting any violations to the DAA for appropriate action.

Naval Air Station Pensacola
Automated Information Systems (AIS) Security
Briefing/User Agreement/Authorization Form

___________________________________ _____________ ______ ____________________
Print: Last Name, First Name, MI   Rank/Rate   Service SSN

Security Briefing: **By Authority of NASPNCLAINST 5239.2B**

1. **Purpose**: To emphasize individual responsibilities pertinent to all NAS Pensacola AIS's.

2. **General**: The protection of sensitive unclassified information is based upon the principles of individual responsibility and accountability. AIS security, like all other security disciplines, depends upon each individual.

3. **Responsibilities**: The responsibility for the security of information used within NAS Pensacola AIS's rests with each user. Regardless of the countermeasures established to protect confidentiality, preserve the integrity, or ensure the availability of the AIS's, networks or the data processed, they provide little security if ignored by individual users. The following AIS User Agreement outlines basic safeguards which must be closely followed when using NAS Pensacola AIS assets.

4. **Action**: All users will adhere to the following guidelines. Failure to strictly comply with these guidelines could result in administrative and/or disciplinary action.

AIS USER AGREEMENT

I UNDERSTAND THAT:

- Failure to sign this agreement will result in denial of access to NAS Pensacola AIS's.
- The use of NAS Pensacola automated resources is strictly limited to **official** command business.
- I will protect my password(s) at the highest level of data it secures and not divulge it to anyone except as may be required by the Information Systems Security Manager (ISSM) or the Information Systems Security Officer (ISSO).
- All magnetic media must be properly stored and labeled.
- Any attempt to circumvent AIS security safeguards will result in immediate revocation of my AIS access and may be referred for administrative or punitive actions.
- I will not attempt to break into or compromise the network or any connected AIS(s) to gain access to data for which I am not specifically authorized.
- I will immediately report any suspected or real violation of AIS security, or any other inappropriate activity I observe directly to the ISSO or ISSM.
- Posting to an INTERNET site requires prior approval.
- Access to INTERNET is authorized only for the performance of **official duties. No** games, software that violates copyright laws, obscene or offensive data files, or other material specifically prohibited may be downloaded or uploaded to the INTERNET.
- All AIS's are subject to authorized monitoring to ensure system functionality to verify the application of prescribed security countermeasures, and to protect against unauthorized use.
- If monitoring reveals possible evidence of criminal activity, such evidence may be provided to appropriate law enforcement personnel.
- By my signature, I expressly consent to monitoring.

I AGREE TO:

- Use only those command AIS resources which I am authorized to access and only for the purposes for which they were intended.
- Not circumvent any AIS security countermeasures or safeguards.
- Not probe or attempt to break in or gain access to any AIS, network, node, or account which I am not authorized access.
- Properly logoff the AIS upon completion of work or departing the immediate terminal area for any length of time.
- Handle all magnetic media and AIS generated printed material in accordance with existing instruction.
- Not download or transmit software which violates copyright laws, obscene or offensive data files, or other material specifically prohibited by NASPNCLAINST 5239.2B.
- Familiarize myself with NASPNCLAINST 5239.2B which specifically deals with INTERNET Connectivity and sign the associated user agreement prior to accessing INTERNET.
- Report any weaknesses in AIS countermeasures or procedures I observe or encounter to the ISSO or ISSM.

_______________________________ ____________
Signature Date

AIS USER AUTHORIZATION:

In consideration of your acknowledged understanding of basic AIS security practices and procedures, you are hereby authorized limited access to operate and use NAS Pensacola AIS resources necessary to perform your duties.

Attempts to probe or break in to other systems or accounts, circumvent internal protection, accounting or auditing mechanisms, or use AIS assets for purposes other than which they were intended or accredited, will be reported as security violations and as a breach of this lawful order.

All NAS Pensacola AIS's are to be used for **Official Government business only** by authorized users. Individual user activities on AIS's are subject to authorized monitoring without notice by system management or AIS security personnel. Anyone using AIS's expressly consents to such monitoring and is aware that if monitoring reveals evidence of user misfeasance, he or she will be subject to appropriate disciplinary action.

____
Information Systems Security Officer/System Administrator

Privacy Act Statement: Authority to request this information is contained in 5 U.S.C. Statue 301 for the purpose of requesting information to ensure NAS Pensacola military, civilian, and contractor personnel who have signed this security briefing/user agreement form are correctly identified. Disclosure is voluntary; however, failure to disclosure will result in your access to AIS resources being denied.